How to audit findings in third-party code

This page has been made public for vendors

Question

The Fortify scan has identified potential issues in third-party code, where the third-party code may or may not be listed in the TRM. What is the appropriate way to audit these findings?

Answer

It is common to include third-party libraries (especially Javascript libraries and frameworks such as jquery or backbone.js) in the Fortify scan. Fortify will report any potential vulnerabilities it detects in that third-party code.

Vulnerabilities in the third-party libraries used by an application are vulnerabilities in that application. Therefore, developers are expected to audit all findings identified by Fortify in these third-party libraries. Developers should evaluate whether or not the identified finding is a true positive and provide detailed comments for any false positives. Reviewers will evaluate the developer comments in the same manner as the comments against findings in the application code. A statement that the finding is in third-party code will not be considered an acceptable comment.

Any critical and high true positives identified in the third-party code are expected to be mitigated. If these mitigations cannot be implemented in the third-party code by for example updating the third-party code to its latest version, the application code should be modified to mitigate the concern.

The software assurance program office is not able to provide a list of known false positives from commonly scanned third-party code. The validity of many findings reported by Fortify depends on how the libraries are used by the application so they must be evaluated in the context of each application.

References

- VA Secure Code Review SOP

HPE Fortify Version	4.42 and later
Programming Language	☐ C/C++ ☐ .NET ☐ Java ☐ Objective-C ☑ Other
Fortify Audit Workbench	☐ Yes ☑ No
Fortify IDE Plugin	☐ Yes ☑ No
Other Fortify Component	☑ Yes ☐ No

Request code review tools, validations, and support HERE.